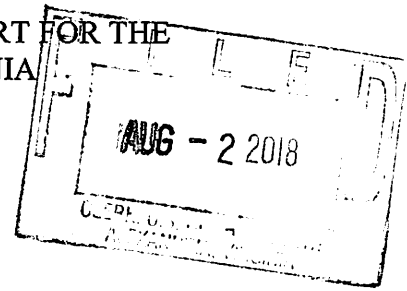


IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

v.

Case No. 1:18-MJ-377

HARES FAKOOR,

**Filed Under Seal**

Defendant.

**AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT AND ARREST WARRANT**

I, Tonya Sturgill Griffith, being duly sworn, depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been so employed since in or around February 2002. I currently am assigned to the Washington Field Office, and I am part of the Northern Virginia–Washington, D.C. Internet Crimes Against Children Task Force. Since joining the FBI, I have investigated violations of federal law involving organized crime, drug trafficking, extra-territorial crime, and terrorism, as well as child exploitation and child pornography offenses.

2. As a Special Agent with the FBI, I have basic and on-the-job training in the investigative area of child exploitation and child pornography. I have participated in federal, multi-jurisdictional, and international investigations. I also am authorized to execute warrants issued under the authority of the United States, and I have participated in numerous search warrants, many of which involved child exploitation and/or child pornography.

3. As a federal agent, I am authorized to investigate violations of the laws of the United States. Since 2010, I have investigated criminal violations relating to child exploitation

and child pornography, including violations pertaining to the illegal production, distribution, receipt, advertisement, presentation, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media.

4. This Affidavit is submitted in support of a criminal complaint and arrest warrant charging **HARES FAKOOR** of Aldie, Virginia, with receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1). For the reasons set forth below, I submit that probable cause exists to believe that between in or about January 2016, **FAKOOR** knowingly received child pornography in Aldie, Virginia, which is within the Eastern District of Virginia.

5. The statements contained in this Affidavit are based on my experience and background as a Special Agent working in the area of child exploitation and child pornography, on information provided by other law enforcement agents and other individuals, and on my review of reports and records. I have not set forth every fact resulting from the investigation; rather, I have set forth the facts necessary to establish probable cause for the requested complaint and arrest warrant.

#### **STATUTORY AUTHORITY AND DEFINITIONS**

6. Title 18, U.S. Code, Section 2252(a)(2) prohibits the knowing distribution and receipt of any visual depiction of minors engaging in sexually explicit conduct using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer. For

purposes of this affidavit, “visual depiction[s] of minors engaging in sexually explicit conduct,” will be referred to as “child pornography.”

7. The term “minor,” as defined in 18 U.S.C. § 2256(1), means any person under the age of 18 years.

8. The term “sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2)(A)(i)–(v), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

9. The term “visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data that is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

### **BACKGROUND TO THE INVESTIGATION**

10. The subject of the underlying investigation is the sharing of images and videos depicting child pornography via a peer-to-peer (“P2P”) file sharing network. As described below, I submit that probable cause exists to believe that between in or about January 2016, in the Eastern District of Virginia, Hares **FAKOOR** used one or more P2P file sharing networks to knowingly receive child pornography at his residence in Aldie, Virginia, which is within the Eastern District of Virginia.

#### **I. Background on P2P File Sharing Networks and Torrent Files**

11. Based on my training and experience, I know that P2P file sharing is a method of communication available to Internet users through the use of special software programs or

clients. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to transfer digital files from one computer system to another while connected to a network over the internet.

12. I also know that there are multiple types of P2P file sharing networks on the internet. To connect to a particular P2P file sharing network, a user first chooses to download from the internet a P2P client software program for a particular P2P file sharing network. Moreover, I know that a particular P2P file sharing network may have many different P2P client software programs that allow access to that particular P2P file sharing network or multiple P2P file sharing networks. These P2P client software programs share common protocols for network access and file sharing.

13. I also know from my training and experience that P2P client software allows the user to set up files on a computer to be shared on a P2P file sharing network with other users on the network. A user also can obtain files by opening the P2P client software on the user's computer and conducting a search for files that are of interest and currently being shared on a P2P file sharing network.

14. The BitTorrent network is a file sharing network that operates over the internet. Users of the BitTorrent network use "torrent" files to search for and obtain desired files. A torrent file is a small file that contains information about one or more other, different files. A user may conduct text or keyword searches on an internet site to locate a torrent file and then, after locating the torrent file, download it. The user can then use that torrent file on a P2P network to locate other users who are sharing the other file (or files) to which the torrent file refers. For example, a person looking to download a music file containing a particular song may conduct internet searches to find a torrent file that is associated with that song. After

downloading the torrent file, the person can use the torrent file to find other people who are sharing that song over a P2P network. After doing so, that person may be able download the song file itself through the P2P network. The same process also applies to video and image files, including images and video of child pornography.

## **II. Undercover P2P Downloads in 2015 and 2016**

15. On or about July 15, 2015, I used a law enforcement tool to identify Internet Protocol (“IP”) addresses that had recently been recorded as sharing, via the BitTorrent P2P file sharing network, images or videos known to law enforcement to be consistent with child pornography.

16. One of the IP addresses identified by the law enforcement tool was 108.48.83.51 (hereinafter, the “SUBJECT IP 1”). Because the law enforcement tool also indicated that SUBJECT IP 1 was connected to the BitTorrent network, also on or about July 15, 2015 through July 18, 2015, I connected to SUBJECT IP 1 over the BitTorrent network. I identified files with names indicative of child pornography and attempted to initiate single source downloads so as to obtain the files exclusively from SUBJECT IP 1. Specifically, I observed that SUBJECT IP 1 was making available for download a torrent file that referred to multiple files with file names that include “((Hussyfan)) Mylola Info Vika Hard.avi,” “(Pthc) Open 33 – 9Yo & 11Yo Girls Play With Dad’s Dick.mpg,” “[PTSC] (video-nymphets,ukrainian young angels)av-005.avi,” and “LolitaSex Movie – Best Teens – Marianna – Danish teen 14yo fucked outside – Holland porno 1 (full 32m 16s) [Lolita Network – NL].mpg.”

17. Through the downloads from SUBJECT IP 1 on or about July 15 through July 18, 2015, law enforcement successfully obtained several files of suspected child pornography, including:

- a. An image identified as “((Hussyfan)) Mylola Info Vika Hard.avi\_000708958.jpg,” which depicts what appears to be a nude minor girl sitting on a bed with her legs spread and with a hot dog in her mouth. The girl’s leg are positioned so that her vagina is blocked from view, but her left breast is visible.
- b. An image identified as “((Hussyfan)) Mylola Info Vika Hard.avi\_0007700838.jpg,” which is a close-up image of what appears to be a minor girl’s vagina and her hand inserting a hot dog into her vagina. The girl appears to be sitting on a bedspread that matches the bedspread visible in the above image, titled “((Hussfan)) Mylola Info Vika Hard.avi\_000708958.jpg.”
- c. An image identified as “(Pthc) Open 33 – 9Yo & 11Yo Girls Play With Dad’s Dick.mpg\_000305400.jpg,” which depicts what appears to be an adult male, who is nude from the waist down, standing with his erect penis in front of what appears to be a clothed minor girl, who is sitting on her knees in front of the adult male and facing him.

18. On or about July 18, 2015, again using a law enforcement tool, I again identified SUBJECT IP 1 as making files of suspected child pornography available for download. Because the law enforcement tool indicated that SUBJECT IP 1 was connected to the BitTorrent network, also on or about July 18, 2015, I connected to SUBJECT IP 1 over the BitTorrent network. I identified files with names indicative of child pornography and attempted to initiate single source downloads so as to obtain the files exclusively from SUBJECT IP 1. Specifically, I observed that SUBJECT IP 1 was making available for download a torrent file named “LS Island-Land-

Midsummer-Touch-Hots, etc LS [9 Sets],” that referred to, among other things, several sets of image files, each containing approximately one hundred or more images, and a document titled “An insight into Child Porn.txt.” I was unable to complete downloads of any of these files.

19. Law enforcement later determined through an open source Internet research tool that SUBJECT IP 1 resolved to Verizon, an Internet service provider. Records obtained from Verizon revealed that, during the time of the activity discussed above in Paragraphs 19-21, SUBJECT IP 1 was assigned to a residence in Aldie, Virginia (hereinafter, the “SUBJECT PREMISES”), which is located within the Eastern District of Virginia. Verizon’s records also indicated that the subscriber for the Verizon account associated with SUBJECT IP 1 was a relative of **FAKOOR**’s.

20. On or about January 31, 2016, I again used a law enforcement tool to identify IP addresses that recently had been recorded as sharing, via the BitTorrent P2P file sharing network, images or videos known to law enforcement to be consistent with child pornography.

21. One of the IP addresses identified by the law enforcement tool was 72.66.71.90 (hereinafter, the “SUBJECT IP 2”). Because the law enforcement tool also indicated that SUBJECT IP 2 was connected to the BitTorrent network, also on or about January 31 through February 1, 2016, I connected to SUBJECT IP 2 over the BitTorrent network. I identified files with names indicative of child pornography and initiated single source downloads so as to obtain the files exclusively from SUBJECT IP 2.

22. Through the downloads from SUBJECT IP 2 on or about January 31 through February 1, 2016, law enforcement successfully obtained several video and image files of suspected child pornography, including:

- a. A video identified as “(PT) ' ' lhannah\_fondle=a3.avi,” which depicts

what appears to be an adult male's hand pulling down the pants of a prepubescent girl, rubbing the girl's vagina, and then picking up the girl to move her closer to the camera;

- b. A video identified as "Claudia 12 anos.avi," which depicts a nude prepubescent girl masturbating on a bed; and
- c. A video identified as "1Hannah\_a8\_forced\_h.mpg," which depicts an adult male spreading the legs of a prepubescent girl to expose her anus and vagina, and then spreading the girl's labia to expose her genitals.<sup>1</sup>

23. Law enforcement determined through an open source Internet research tool that SUBJECT IP 2 resolved to Verizon, an Internet service provider. Records obtained from Verizon revealed that, during the time of the downloads discussed above in Paragraphs 21-22, SUBJECT IP 2 was also assigned to the SUBJECT PREMISES and that the subscriber for the Verizon account associated with SUBJECT IP 2 was the same relative of **FAKOOR's**.

### **III. Execution of a Search Warrant in May 2016 and Forensic Examinations of FAKOOR's Devices**

24. On or about May 13, 2016, law enforcement agents executed a federal search warrant, which had been issued by the U.S. District Court for the Eastern District of Virginia, on the SUBJECT PREMISES. At the time the search warrant was executed, **FAKOOR** and a number of other individuals were at the residence. Law enforcement informed the occupants of

---

<sup>1</sup> The files described in this paragraph, which law enforcement downloaded from the SUBJECT IP 2 in January and February 2016, appear to have been inadvertently deleted during the course of a routine backup of an FBI device after the execution of the search warrant. The descriptions of the files provided in this affidavit are based on my prior review of these files and a prior affidavit I prepared as part of this investigation before the files were deleted. Additionally, as explained below, law enforcement seized a laptop from **FAKOOR's** room that contained files with these same titles and meeting these same descriptions.



the nature of the investigation.

25. The warrant authorized a search of the premises for evidence of child pornography, and, pursuant to the warrant, law enforcement seized several digital items, including a HP Envy 700 PC Desktop computer (Serial # MXX5190M41) (hereinafter referred to as the “HP”), which was seized from **FAKOOR**’s bedroom.

26. Law enforcement personnel conducted a computer forensic examination of the seized devices, including the HP. This examination revealed that the HP contained a password-protected user account folder called “Hares.” When the forensic examiner booted up the HP as a virtual machine, the login screen associated with the “Hares” account folder also listed the name “Hares Fakoor” and the email address “haresfakoor@outlook.com.”

27. Within the “Hares” account were the file-sharing programs BitComet and uTorrent, both of which operate over the BitTorrent P2P network. The uTorrent program on the HP was configured to connect with a proxy server “proxy.torguard.org.” TorGuard is a service that provides anonymous proxy services to mask a user’s IP address when accessing the internet. Specifically, a user can configure the uTorrent program to utilize a TorGuard proxy while downloading and sharing files through uTorrent. With regard to the uTorrent program on the HP, the username associated with the TorGuard proxy in the uTorrent settings was “hfakoor2@gmu.edu.” (**FAKOOR** attended George Mason University.)

28. The forensic examination of the files stored on the HP’s hard drive under the “Hares” user account included hundreds of videos and images that depict children engaged in sexually explicit conduct. This determination was based on several factors, including the lack of pubic hair, the physical development of genitalia, and the lack of breast development of the minors depicted in the videos and images.

29. Among the files found within the “Hares” user account on the HP were child pornography files downloaded via the BitTorrent network or torrent files with names suggestive of child pornography. For example, the forensic examiner found the following on the HP:

- a. On January 10, 2016, the user of the HP typed the terms “pthc,” “ptsc,” and “pedo” into a field on a website. In my training and experience, these terms, respectively, refer to “pre-teen hard core,” “pre-teen soft core,” and “pedophile,” and they are all search terms that are commonly used by child pornography offenders. Shortly afterward, the user visited a torrent-based website and downloaded two torrent files entitled “new 2008 9yo preteen gay boy child first private sex pthc pedo kiddie cum.torrent” and “pthc jenny 9yo.torrent” to the “\Users\Hares\Downloads\” folder on the HP. These torrent files were still in this folder at the time that the forensic examiner conducted the examination, and both of them had creation and last written dates of January 10, 2016.
- b. The HP also contained a folder “\Users\Hares\Downloads\รวมคลิป loli 4” that contained several video files depicting child pornography with file creation dates of January 10, 2016. For example, the files in this folder included a video titled “Jenny 9Yo Zoo 5Yo Girl Dog And.avi,” which depicts a dog licking the vagina of a naked prepubescent girl who is blindfolded and bound with yellow rope. Later in the video, the minor female performs oral sex on what appears to be an adult male. The HP also contained a torrent file entitled “รวมคลิป loli 4.torrent,” created on January 10, 2016 and located in the “\Users\Hares\AppData\Roaming\utorrent”

folder, which is a folder created by the uTorrent P2P file-sharing program. As noted above, uTorrent is a client program for the BitTorrent network. In my training and experience “loli” is short for “Lolita,” which is a search term commonly used by child pornography offenders.

- c. The HP contained a folder “\Downloads\preview\” that in turn contained numerous videos of children being sexually abused, including the videos described above in Paragraph 22. The file names and file sizes in this folder match exactly the file names and sizes associated with a torrent file “preview.torrent,” which was found on the HP within a folder associated with the BitComet program, which as noted above is a client program used to access the BitTorrent network. The “preview.torrent” file listed a creation date of January 28, 2016. Another file generated by the BitComet program indicates that the content associated with the “preview.torrent” file was also downloaded through BitComet on January 28, 2016.

30. Additionally, the folder “\Users\Hares\Downloads\” on the HP included child-pornography-related files intermingled with files that appear to be **FAKOOR**’s personal documents. For example, this folder contained a video file entitled “Kingpass S MNirouf 5-9Myloia 2Girls 11-12Yo Preteen Lolita.avi” that depicts two girls who are approximately 11-14 years old removing their clothes and, among other things, engaging in oral sex. In addition, this folder contained the “new 2008 9yo preteen gay boy child first private sex pthc pedo kiddie cum.torrent” and “pthc jenny 9yo.torrent” files, and its subfolders include the “preview” and “รวมคลิป loli 4” folders. In addition, this “\Users\Hares\Downloads\” folder also contained a Word document entitled “HFakoor Resume.doc,” which is a resume for **FAKOOR** that also lists

his email address as “hfakoor2@gmu.edu.” The folder also contained a number of work-related documents bearing **FAKOOR**’s name as well as the name of an engineering company that, according to “HFakoor Resume.doc,” employed **FAKOOR**.

31. Another folder on the HP, “\Users\Hares\Desktop\Hares Transfer\,” likewise contained child-pornography-related files intermingled with **FAKOOR**’s personal documents. That folder contained a subfolder entitled “\Nn\_Models\NoNude\,” that, despite its name, contained subfolders containing numerous images of children lasciviously exhibiting their naked and clothed genitals, as well as significant amounts of child erotica. The “\Hares Transfer\” folder also contained a subfolder “\Resume\,” which contained additional copies of **FAKOOR**’s resume, as well as cover letters for job applications that bear **FAKOOR**’s name.

32. The HP also contained numerous files with the extension “.lnk,” which signify that a user of the computer has opened another file on the computer. A number of the .lnk files have titles that are consistent with child pornography files being viewed, such as “Daughters-girls from 12yo to 14yo having sex experiences (Hussyfan) (pthc) (r@ygold)underage.mpg.lnk,” “(Pthc) NF\_vid\_006 Piet and Fred 2 boys 13yo and 10 fuck and suck. 10yo has dry orgasm – preteen pedo gay kiddy.mpg.lnk,” “[ PTHC – Kingpass – Hussyfan] Mary 7Yo Arab Girl.mpg.lnk,” and “[March 2014] (Hussyfan) (pthc) (r@ygold) Preteen Asian ALICA, 11yo Philippine ( Filipina ) child prostitute XXX HC Pedo ptsc.rar.rar.bc!.lnk.” The .lnk files with names suggestive of child pornography or child erotica have last written dates between approximately December 2015 and May 2016, which indicates when the associated files were accessed.

### CONCLUSION

33. Based on the above information, I respectfully submit that there is probable cause to believe that between in or about January 2016, in the Eastern District of Virginia, **HARES**

**FAKOOR** knowingly received child pornography in violation of 18 U.S.C. § 2252(a)(2) and (b)(1). Therefore, I respectfully request that a criminal complaint and arrest warrant be issued for **FAKOOR**.

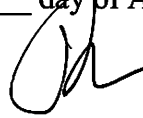
Respectfully submitted,



Tonya Sturgill Griffith, Special Agent  
Federal Bureau of Investigation

Sworn and subscribed before me  
this 2 day of August 2018

/s/



Theresa Carroll Buchanan  
United States Magistrate Judge

The Honorable Theresa Carroll Buchanan  
UNITED STATES MAGISTRATE JUDGE